

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENT	vii
	LIST OF TABLES	x
	LIST OF FIGURES	xi
	LIST OF ABBREVIATIONS	xii
1	INTRODUCTION	1
	1.1 Introduction	1
	1.2 Evolution of Spam and Ways to Filter	1
	1.3 Problem Statement	3
	1.3.1 Limitations of Bayesian	3
	1.3.1.1. Image Spam	5
	1.3.1.2. Open Relay and Proxies	6
	1.3.1.3. Botnets	7
	1.3.1.4. Spam with Dynamic Contents	8
	1.3.2 Available Solution in Resolving Issues with Bayesian	8
	1.4 Definition of Patterns	9

1.5	Objective	10
1.6	Scope	12
1.7	Hardware Specification for Simulation	13
1.8	Summary	13
2	LITERATURE REVIEW	14
2.1	Introduction	14
2.2	Antispam Solutions without Bayesian	14
2.2.1	Image Spam	15
2.2.2	Botnets and Network Level Protection	17
2.2.3	Dynamic Contents	23
2.3	Antispam with Bayesian	26
2.4	Summary	27
3	METHODOLOGY	29
3.1	Introduction	29
3.2	Methodology	29
3.2.1	Traffic Shaping	30
3.2.2	Sender Reputation	31
3.2.3	Sender Policy Framework	31
3.2.4	DNS Blacklist (DNSBL)	33
3.2.5	Recipient Validation	34
3.3	Improvement To Expect	34
3.4	Sample Data	35
3.5	Requirement for the simulation	36
3.5.1	Development Tool	36
3.5.2	Prototyping	37
3.5.3	Implementation	54
3.5.4	Simulation Environment	54
3.6	Test Methodology	55
3.7	Summary	56

4	RESULT AND ANALYSIS	60
	4.1. Introduction	60
	4.2. Result	60
	4.3. Analysis	66
	4.4. Conclusion	67
5	DISCUSSION	68
	5.1 Introduction	68
	5.2 Discussion	68
	5.3 Conclusion	69
6	CONCLUSION	70
	6.1 Introduction	70
	6.2 Conclusion Remarks	70
	6.3 Future Work	71
	REFERENCES	73

LIST OF TABLES

TABLE NO.	TITLE	PAGE
1.1	Specification of The Computer For The Simulation	13
2.1	Comparison of Methods to Detect Image Spam	17
2.2	Comparison of Network-Level Protection Techniques	22
2.3	Comparison of Techniques to Cater For Dynamic Contents	26
2.4	Recommended Combination for Pattern-Based Filtering Technique	27
2.5	Recommended Combination for Pattern-Based Filtering Technique (Continue)	28
4.1.	Result of ASPBF	64
4.2.	Result of Antispam without ASPBF	65

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.1	Sample of Image Spam	5
1.2	Architecture of EMP	8
2.1	Sample of Distorted Text in Image	15
2.2	Examples of spam images	16
3.1	System Architecture (part 1)	32
3.2	System Architecture (part 2)	33
3.3	Function of Traffic Shaping (Part 1)	37
3.4	Function of Traffic Shaping (Part 2)	38
3.5	Function of Sender Reputation (Part 1)	38
3.6	Function of Sender Reputation (Part 2)	39
3.7	Function of Sender Reputation (Part 3)	40
3.8	Function of Sender Reputation (Part 4)	41
3.9	Function of Sender Reputation (Part 5)	42
3.10	Function of Sender Reputation (Part 6)	43
3.11	Function of Sender Reputation (Part 7)	44
3.12	Function of Sender Policy Framework (Part 1)	45
3.13	Function of Sender Policy Framework (Part 2)	46
3.14	Function of Sender Policy Framework (Part 3)	47
3.15	Function of Sender Policy Framework (Part 4)	48
3.16	Function of DNS Blacklist (Part 1)	49
3.17	Function of DNS Blacklist (Part 2)	50
3.18	Function of DNS Blacklist (Part 3)	51

3.19	Function of DNS Blacklist (Part 4)	52
3.20	Function of DNS Blacklist (Part 1)	52
3.21	Function of DNS Blacklist (Part 2)	53
3.22	Function of DNS Blacklist (Part 3)	54
3.23	Placement of the test components	56
4.1	Logs For DNSBL Filter	59
4.2	Logs For SPF Filter	60
4.3	Logs For Recipient Validation Filter	61
4.4	Logs For Sender Reputation Filter	62
4.5	Logs For Traffic Shaping Filter	63
4.6	Result of Filter with ASPBF	64
4.7	Result of Filter Without ASPBF	65
5.1	Expected outcome from the combination of ASPBF and Bayesian	69

LIST OF ABBREVIATIONS

ASPF	-	Antispam with Pattern-Based Filter
Botnet	-	Robot Network
CNC	-	Cloudmark Network Classifier
CPU	-	Central Processing Unit
DCOM	-	Distributed Component Object Model
DKIM	-	DomainKeys Identified Mail
DNS	-	Domain Name Service
DNSBL	-	Domain Name Service Black Listing
E-Mail	-	Electronic Mail
EMP	-	Extensible Messagin Platform
IP	-	Internet Protocol
LDAP	-	Lightweight Directory Access Protocol
LSASS	-	Local Security Authentication Server
OCR	-	Optical Character Recognition
RAM	-	Random Access Memory
SMTP	-	Simple Mail Transfer Protocol
SPF	-	Sender Policy Framework
SVM	-	Support Vector Machine